Brooklyn Law Review

Volume 80 | Issue 2 Article 8

2015

Electronic Health Records: How to Suture the Gap Between Privacy and Efficient Delivery of Healthcare

Mallory Turk

Electronic Health Records

HOW TO SUTURE THE GAP BETWEEN PRIVACY AND EFFICIENT DELIVERY OF HEALTHCARE

INTRODUCTION

For the past fifty years, electronic healthcare (E-Health) has been a rapidly growing industry. With new innovations came more accessibility for doctors and health providers to retrieve patient data from almost anywhere, and to give patients access to their own information. The growth of electronic healthcare will set up other opportunities, such as decreased costs[1] and increased access to healthcare.[2]

One recent innovation in healthcare is the Electronic Health Record (EHR), which is defined by the Centers for Medicare and Medicaid Services as "an electronic version of a patient's medical history that is maintained by the provider over time, and may include all of the key administrative clinical data relevant to that person's care under a particular provider . . . ."[3] This clinical data may include immunizations, reports, prescriptions, familial history, and anything that may assist in health care maintenance.[4] The data also includes the patient's electronic medical record, which has less detailed information than that in EHRs.[5]

Although various studies reveal that the implementation of EHRs will be beneficial,[6] many are concerned with the lack of

---

[1] Randolph C. Barrows Jr., M.D. & Paul D. Clayton, Ph.D., *Privacy, Confidentiality, and Electronic Medical Records* 3 JAMIA 139, 147 (1996)

[2] *Id.* at 139.

[3] E-HEALTH, PRIVACY, AND SECURITY LAW 2 (W. Andrew H. Gantt III ed., 2d ed. 2011) (citing Ctrs. for Medicare & Medicaid Servs., *Electronic Health Records*, CMS.GOV, http://www.cms.gov/ehealthrecords/ (last updated Mar. 26, 2012)).

[4] BYRON HAMILTON, ELECTRONIC HEALTH RECORDS 4 (2d ed. 2010).

[5] *Id.*

[6] *Analytics in Healthcare*, SAS 3 (2009); *see, e.g.*, Julia Adler-Milstein, Ph.D. et al., *Effect of Electronic Health Records on Health Care Costs: Longitudinal Comparative Evidence From Community Practices*, 159 ANNALS OF INTERNAL MEDICINE 97, 103 (2013); Samuel J. Wang, M.D., Ph.D. et al., *A Cost-Benefit Analysis of Electronic Medical Records in Primary Care*, 114 AM. J. MED. 397, 401 (2003).

privacy and the threat of potential breaches.[7] Computer hackers can break into storage database and access patient records.[8] Further, if a patient generally asks for "all [of her] health information", a doctor may accidentally disclose sensitive information that they may not legally release.[9]

In 2009, Congress passed the American Recovery and Reinvestment Act[10], which expands the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to include all "business associates" within its security and privacy provisions.[11] HIPAA was enacted in 1996 to better protect patient information through increased security and privacy standards for information that could be linked to a specific patient.[12] After the implementation of the American Recovery and Reinvestment Act, the Department of Health and Human Services (HHS) established new regulations[13] that standardize how EHRs must be set up.

Despite Congressional efforts to protect patient privacy, there are still privacy issues that must be addressed. With the increase of computer hacking[14] and accidental releases of private information, there are continued concerns with security until the patients know that the people protecting their records are doing so to the best of their ability. Congress has placed safeguards to try to protect patient information. These safeguards include encrypting information,[15] de-identifying specific patient information when storing health records,[16] and recording each time an EHR is accessed.[17] Some of these safeguards are included in the criteria that the creators of EHRs, private companies that

---

[7] *See, e.g.*, Barrows, *supra* note 1, at 139.

[8] *HIPAA Regulatory Alert: Computer Hackers Step Up Attacks on Health Care Records*, AHC NEWSLETTERS (May 20, 2008), http://insurancenewsnet.com/oarticle/2008/05/20/hipaa-regulatory-alert-computer-hackers-step-up-attacks-on-health-care-records-a-94434.html#.UtmMchb0Ay4.

[9] Donnaline Richman, *Legal Pitfalls of Electronic Medical Records*, DATELINE: A NEWSL. FOR MLMIC-INSURED PHYSICIANS, DENTISTS, & FACILITIES (MLMIC, New York, N.Y.), Fall 2013, at 6.

[10] American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (2009).

[11] *Id.* § 13401; *see also* Corrine P. Parver, Esq. & Savannah Thompson-Hoffman, *On the Front Lines*: *How the American Recovery and Reinvestment Act of 2009 Changed HIPPA's Privacy Requirements*, CCH HEALTH CARE COMPLIANCE LETTER 1, 4 (July 28, 2009).

[12] Diane Kutzko et al., *HIPAA in Real Time: Practical Implications of the Federal Privacy Rule*, 51 DRAKE L. REV. 403, 407 (2003).

[13] 45 C.F.R. § 170.314 (2012).

[14] *See infra* text accompanying notes 25-30.

[15] 45 C.F.R. §§ 170.210(a); 170.302(s)-(v).

[16] *Id.* § 164.514(a).

[17] *Id.* § 170.210(b).

develop the software, known as vendors, must meet, but there is little incentive for these vendors to comply. In order to encourage compliance, HHS should impose a civil monetary penalty if the vendors fail to continuously comply with the criteria, similar to one already in place in a different aspect of medical data law. This would require the vendors to pay a substantial fee that would clearly reflect the importance of patient privacy. We are in a new age of sharing medical information, so the law surrounding the exchange of health information needs to reflect this, which is what a civil monetary penalty would do.

Part I of this note provides some background on EHRs, exploring the benefits and accompanying risks of EHRs. Part II explains the complex set-up and certification process of EHR software by HHS. It then argues that this certification is not enough by comparing EHR software certification to credit card certification. Part III will look at an existing civil monetary penalty and then explain why that penalty should also apply to vendors of health information technology. This penalty should be a sliding scale so that it is proportional to the vendor's failure to comply with privacy regulations. In assessing the penalty, regulations should consider various factors such as the length of time the certification requirements were not met and the detectability of such failure. Part IV will strengthen the argument to expand the civil monetary penalty through an analysis of the effects of its imposition. This will show that the implementation of the penalty is not only better for patients than the mere certification process, but is also better for medical facilities and the vendors themselves.

I. BACKGROUND

A. Explanation of EHRs

EHRs, very basically, are a way to store and transfer patient information. EHRs store three types of data: quantitative, qualitative, and transactional. Quantitative data is information that is dependent on the individual patient, such as laboratory values that are inputted after doctors review test results. Qualitative data is information that will not change from patient-to-patient, such as text-based documents, like medical books and demographics. Lastly, transactional data is information that

tracks transactions from the medical provider to the patient, and vice versa, such as medication that has been delivered.[18]

One benefit of EHRs is that they ease access to information. Patients and doctors are not bound to a single paper chart; the information is accessible almost instantaneously from almost any web-based device.[19] Instead of spending time searching in a record room for an individual patient's file, doctors can sit down with the patient at a computer and immediately access all of the patient's medical information. As a result of using a computer, the information is kept up to date because of immediate entry into the system when the data is discovered.[20] When test results come back to the primary doctor, that doctor no longer has to make the extra effort to include the results in a paper chart. Instead, the laboratory doctors would have already placed the results in the patient's record after they found the results. Due to the easy access of EHRs on a computer, doctors no longer need to be in the office to access records. They can write prescriptions, look up patients' charts, and view the status of a particular patient from almost anywhere as long as their device has access to their practice's EHR database.[21]

A familiar stereotype about doctors is that they have terrible handwriting.[22] Another benefit of inputting information into a computer is that it makes the information legible. This guarantees that the medical charts and all other information in the EHR are clear. Clarity of patient information leads to less confusion and avoids possible mistakes as a result of an illegible health record.[23] Further, hospital discharge notices are created for the individual patient based on his or her individual ailments and prescriptions. EHRs also make it easier to quickly identify which patients have been prescribed recalled drugs and decrease the likelihood of misplaced or lost lab work because the information is stored on a single database.[24]

Despite these benefits, the implementation of EHRs raises significant privacy concerns due to potential security

---

[18] Travis B. Murdoch, M.D., MSc & Allan S. Detsky, M.D., Ph.D., *The Inevitable Application of Big Data to Health Care*, 309 JAMA 1351, 1351 (2013).

[19] Introduction to Electronic Health Records, THE MCGRAW-HILL COMPANIES 8 (2011).

[20] *Id*.

[21] *Id.*

[22] Donald M. Berwick & David E. Winickoff, *The Truth About Doctors' Handwriting: A Prospective Study*, 313 BMJ 1657, 1657 (1996), *available at* http://bmj.com/content/313/7072/1657.

[23] *An Introduction to Electronic Health Records*, *supra* note 19, at 8.

[24] *Id.* at 9.

vulnerabilities. In a 2012 study, 94% of healthcare organizations reported that they had at least one security breach within the last two years.[25] Forty-five percent of those healthcare organizations that had been breached reported having at least five breaches.[26] This is a substantial increase from a 2010 study where 86% of healthcare organizations reported that they had had at least one security breach in the past two years but only 29% reported that they had more than five.[27] Negligence on the part of those meant to protect EHRs primarily caused these breaches. In 2012, employee mistakes and inactions caused 42% of breaches.[28] The percentage of criminal attacks on information technology security also increased from 20% in 2010 to 33% in 2012, at the time of the study.[29] Moreover, 46% of breaches were a result of lost or stolen devices.[30]

When EHRs are lost or stolen there is a risk of medical identity theft because EHRs include personal health facts, such as names, personal identity, and billing information.[31] This can create a problem because the thief can use this information fraudulently, including to obtain medical services, and prescription drugs, while continuing to bill the victim.[32] Moreover, the personal facts that are found within EHRs, such as illness or genetic traits, can be revealed.[33] This revelation can lead to embarrassment or discrimination.[34] EHR privacy, accordingly, is of the utmost importance.

In addition to privacy concerns, there are several other concerns with the full implementation of EHRs. First, there is no guarantee that doctors will entirely fill out comment sections. Doctors may resort to simply checking the boxes provided instead of taking the time to write detailed information about a specific patient.[35] Even if a doctor decides to include information in the comment section, they may simply repeat what they said

---

[25] PONEMON INST., THIRD ANNUAL BENCHMARK STUDY ON PATIENT PRIVACY & DATA SECURITY 5 (2012), *available at* http://www.ponemon.org/news-2/45.

[26] *Id.*

[27] *Id.*

[28] *Id.* at 2.

[29] *Id.*

[30] *Id.*

[31] *See generally* PONEMON INST., THIRD ANNUAL SURVEY ON MEDICAL IDENTITY THEFT (2012), *available at* http://www.ponemon.org/library/third-annual-survey-on-medical-identity-theft-ponemon-institute.

[32] *Id.* at 1.

[33] PONEMON INST., *supra* note 25, at 2.

[34] Louise Slaughter, *Genetic Information Non-Discrimination Act*, 50 HARV. J. ON LEGIS. 41, 44-45 (2013).

[35] Richman, *supra* note 9, at 2.

on an earlier visit by cutting information from one section and pasting it into a new section, forgetting to include any new information.[36] This negatively impacts the patient because their EHR will not reflect details related to this specific visit; even minor differences may matter in the future. Second, although typed notes are more legible, spelling errors still persist and there are no universal abbreviations.[37] This may make it difficult for a subsequent doctor to clearly understand the patient's medical history or it may affect pharmaceutical information, leading to wrong prescriptions or diagnosing adverse medications. Lastly, EHRs are expensive, even though the price varies depending on the size of the practice and the EHR employed. Some hospitals and healthcare networks can spend at minimum $10 million on setting up the entire system.[38] Smaller group practices may spend anywhere between $10,000 and $20,000 for each doctor they employ.[39] The expense does not stop after the system has been set up. Maintaining the entire system can cost the practices an additional twenty-five percent every year,[40] which could have adverse consequences on practices, especially the smaller practices.

The benefits of EHRs substantially outweigh the downsides, so medical facilities with EHRs are still better off than the alternative. The speed and clarity prevent bigger problems. For example, the only time a doctor will have an incomplete medical history for a patient would be the first time the doctor is implementing EHRs. Once EHRs are already in place, a newborn's medical information would be put into his or her EHR, which would then be accessible, by every subsequent doctor throughout his or her lifetime. Moreover, as detailed later on, EHRs are inevitable.[41] The ability to communicate with different medical providers quickly and with a full and accurate patient medical record is extremely important in today's society.

---

[36] *Id.* at 2-3.

[37] *Id.* at 1.

[38] *Analytics in Healthcare*, *supra* note 6, at 3.

[39] *Id.*

[40] *Id.*

[41] *See infra* text accompanying notes 230-36 (discussing the cohesiveness of EHRs to benefit medical treatment).

B. History of EHRs

EHRs were first used in the 1960s at The Mayo Clinic in Rochester, Minnesota, and the Medical Center Hospital in Vermont.[42] These two facilities implemented EHRs in the hopes that through such use would come easier access to the growing complexity of medicine and medical records.[43] Over the next decade, EHRs further expanded to better "capture [] clinical information."[44] These improved EHRs could now record various information, such as test results, medications, and surgeries.[45] Furthermore, the method of storage changed within this decade as well. At first these separated servers had to stay within a relatively small distance from the facility and the facility kept a backup server on-premise.[46] EHR vendors were no longer constrained to store them within the medical facility. Servers could now be remote, continuing to improve patient privacy.[47]

In the late 1980s, the federal government became involved in the implementation of EHRs, showing its dedication to EHR use as well as EHRs' importance and necessity through subsidizing the growth of EHRs. In 1988, the government awarded a grant to Composite Health Care System to help the company maintain their intricate database, used to store and maintain patient records. This contract was continuously renewed until 1996.[48]

Presidents George W. Bush and Barack Obama have each commented on the importance of EHRs. President Bush stated that he wanted patients to have access to EHRs in order to improve the overall quality of provided healthcare.[49] President Obama said that a stimulus package, specifically targeted to

---

[42] *An Introduction to Electronic Health Records*, *supra* note 19, at 2.

[43] *Id.*

[44] Gilad J. Kuperman, M.D. & Reed M. Gardner, Ph.D., *The Impact of the HELP Computer System on the LDS Hospital Paper Medical Record*, 12 TOP HEALTH REC. MGMT. 76 (1990).

[45] *Id.*

[46] POLICY IMPLICATIONS OF MEDICAL INFORMATION SYSTEMS 21 (1977), *available at* www.princeton.edu/~ota/disk3/1977/7708/770805.PDF.

[47] *Id.* at 26-30.

[48] U.S. GEN. ACCOUNTING OFFICE, GAO/AIMD-96-39, DEFENSE ACHIEVES WORLDWIDE DEPLOYMENT OF COMPOSITE HEALTH CARE SYSTEM 3 (1996), *available at* http://www.gao.gov/assets/230/222364.pdf.

[49] The White House, *Transforming HealthCare: The President's Health Information Technology Plan* (2004), *available at* georgewbush-whitehouse.archives.gov/infocus/technology/economic_policy200404/chap3.html.

improve EHRs, could help prevent errors and save money.[50] In 2009, President Obama stated that ideally all medical records should be computerized in the hopes that not only could they improve healthcare and create jobs, but also save lives.[51]

Today, E-Health is defined as "the use of digital information and communication technologies to improve people's health and health care."[52] The purpose of E-Health is to electronically store patient data, prescribe medication, and allow the patient to have easier access to her own records,[53] which is exactly what EHRs do. Recently, as a result of the 2009 Health Information Technology for Economic and Clinical Health Act, regional health information organizations were set up for health care providers to better communicate within a particular region.[54] The purpose of these regional health information organizations is to bring together various medical providers within a local community to better exchange data.[55] These organizations have been slow-moving in the overall broad exchange of health information.[56]

The 2009 Health Information Technology for Economic and Clinical Health Act set up a three-factor approach to health information exchange.[57] First, the Act states that participation in the health information exchange is part of the criteria for medical facilities to receive federal incentives for using EHRs.[58] Second, the Act encourages states to create affordable options for using and implementing EHRs. HHS set up a four year $548 million State Health Information Exchange Cooperative Agreement Program to ensure that states could set up a system to share medical information.[59] Lastly, the Act supports the Direct Project, which is a system of Internet services, similar to e-mail, used to send and retrieve electronic health information.[60]

---

[50] Robert Pear, *Privacy Issue Complicates Push to Link Medical Data*, N.Y. TIMES, Jan. 18, 2009, at A16, *available at* http://www.nytimes.com/2009/01/18/us/politics/18health.html?_r=0.

[51] *Id.*

[52] U.S. Dep't of Health & Human Servs., *What is e-Health?*, http://health.gov/communication/ehealth/ (last visited Feb. 20, 2015).

[53] E-HEALTH, PRIVACY, AND SECURITY LAW, *supra* note 3, at 2-3; Parver & Thompson-Hoffman, *supra* note 11.

[54] Julia Adler-Milstein, Ph.D. & Ashish K. Jha, M.D., M.P.H., *Sharing Clinical Data Electronically: A Critical Challenge for Fixing the Health Care System*, 307 JAMA 1695, 1695 (2012).

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] *Id.*

[59] *Id.*

[60] *Id.*

The Act assumes that through this original promotion of the secure transfer of information from one provider to another, it will further develop in the future so that there will be no need to transfer data and providers will simply be able to search for and retrieve information on their patients.[61]

C. Types of EHRs

Today, there are two different types of EHRs: cloud-based and on-premise. Cloud-based EHRs, also called "web based" or "Software as a Service," have been increasingly growing in popularity among smaller practices.[62] This model is based in the web, so facilities do not need to install the software on their own computers.[63] To access patient records, the users sign on to a secure Internet browser, which connects the user to the data storage.[64] The vendor is responsible for maintaining the system as well as ensuring security of the records.[65] Instead of charging medical facilities significant costs to set up the EHR system, cloud-based vendors simply charge the facilities an average monthly fee of approximately $200-400.[66]

In addition, patient care quality has substantially increased because of cloud-based EHRs. For example, if a patient who visited a hospital on vacation is released, and the doctor wants to schedule them for a follow up in their hometown, the doctor no longer needs to search for follow up facilities. Rather, the doctor can input the patient's zip code and find facilities through the software and directly contact the providers listed.[67] Moreover, according to facilities that already use this form of software, the implementation and education as to how to properly use these EHRs was relatively easy and quick to learn.[68]

There are issues specifically related to cloud-based vendors. Access to EHRs depends on the vendor's availability. So, if the services are unavailable for any reason, the facilities that rely on the vendor will not be able to access their patients'

---

[61] *Id.*

[62] Ken Terry, *SaaS EHR Model Gains Physician Support*, INFO. WEEK (May 17, 2012), http://www.informationweek.com/healthcare/electronic-medical-records/saas-ehr-model-gains-physician-support/240000562.

[63] Lauren Phillips, *Automating Referrals Aids Discharge Process*, HEALTH MGMT. TECH. (Mar. 2010), http://www.healthmgttech.com/articles/201003/automating-referrals-aids-discharge-processes.php.

[64] *Id.*

[65] *Id.*

[66] Terry, *supra* note 62.

[67] Phillips, *supra* note 63, at 25.

[68] *Id.*

EHRs.[69] For this reason, it is important for these vendors to have an off-site backup server as well to ensure continued access to EHRs.[70] There are also many security risks associated with cloud-based software. Cyber hackers can place "eavesdropping software" within these servers, allowing them access to all private information stored within.[71] According to Samantha Shelton, the Information Security Engineer at the Computer Sciences Corporation, "'[i]nformation on public clouds are susceptible to data brokers and other computer hackers,' due to the multiple tenancies and the ability to access multiple customers' information on the same server."[72] However, the servers that contain all of this private personal information need not be stored in the United States. Because they are cloud-based, they can be stored in any country.[73]

The second type of software is the "on-premise" or "client server". This is the relatively more expensive type of software because the medical facility actually buys the entire software package and installs it onto their computers.[74] The EHR vendors might also have remote access to the software in order to assist the medical facilities if they ever need support.[75] The facility, however, is entirely responsible for maintaining the software, backing up all information, and restoring any lost data.[76] Moreover, the medical facilities are responsible for making certain that the data server complies with HIPAA regulations.[77] An on-premise server appears more expensive than cloud-based software because the facilities that implement on-premise servers pay the entire cost when they purchase the software, exclusive of yearly maintenance fees, whereas cloud-based software has maintenance fees included

---

[69] Priya Das et al., *Cyber-Security Threats and Privacy Controls for Cloud Computing, Emphasizing Software as a Service*, 30 THE COMPUTER & INTERNET LAW. 20, 21 (2013).

[70] *Id.*

[71] *Id.* at 22.

[72] *Id.*

[73] *Id.* Vendors would then need to comply with the foreign country's privacy laws and not necessarily have to comply with our privacy laws. *Id.*

[74] Shahid N. Shah, *Interoperable EMRs for the Small-to Medium-Sized Office: On Being the CIO of Your Practice*, *in* THE BUSINESS OF MEDICAL PRACTICE: TRANSFORMATIONAL HEALTH 2.0 SKILLS FOR DOCTORS 299, 328 (David E. Marcinko & Hope R. Hetico eds., 3d ed., 2011).

[75] *Id.*

[76] *Id.* at 329.

[77] *See* Nefertiti C. duPont, M.D., M.P.H. et al., *Selecting an Electronic Medical Record System for Small Physician Practices*, 70 NC MED. J. 399, 402 (2009) (noting that in the client server model the physicians must maintain a secure data center, unlike the ASP model which is designed to meet HIPAA security rule requirements).

in the monthly fee.[78] Startup-costs for on-premise servers can range from $10,000 to $10 million, with about twenty-five percent in maintenance a year.[79] There are far fewer security problems with on-premise servers because it is easier to know who has access to the servers' information. A cloud-based server, however, may be more desirable for smaller facilities because it does not require high start up costs.[80]

II. THE CERTIFICATION PROCESS

In 2010 HHS set up regulations pertaining to the certification of EHRs.[81] This section will look into the extensive requirements that vendors must incorporate into their software before HHS will certify it to be sold to medical facilities. However, this certification is not permanent;[82] failure to comply with any of the regulations will potentially rescind certification for a short amount of time.[83] Because EHRs and their regulation are relatively new, this section will look into credit card certification as an example as to why mere certification and the rescinding of that certification is not enough. There needs to be smarter deterrence to encourage vendors to continuously comply with regulations and protect patient information.

A. How EHRs are Certified

Before EHRs may be legally used and sold, the EHR software must be certified pursuant to HHS regulations.[84] These regulations set out specific criteria with which each vendor must comply. If the vendors comply with the criteria, the Office of the National Coordinator (ONC) then certifies the software.[85] After certification, medical practices and hospitals may purchase the software. The company can seek complete EHR certification or partial certification, among other forms of Health Information Technology certification that have also been laid out in the law.[86]

---

78 Shah, *supra* note 74, at 329.
79 *Analytics in Healthcare*, *supra* note 6, at 3.
80 Shah, *supra* note 74, at 329.
81 45 C.F.R. § 170.300-170.314 (2012).
82 *Id.* § 170.565.
83 *Id.* § 170.565(h)(3).
84 *Id.* § 170.302.
85 *Id.* § 170.503.
86 *Id.* § 170.510.

To obtain certification, the software must meet the twenty-two specific criteria described within the regulation.[87] Among these criteria, EHRs must automatically generate drug interaction and drug-allergy checks based on the individual patient's medications.[88] Similarly, doctors must also be able to check if drugs are a "formulary or preferred drug."[89] Each patient's record must be able to maintain an ongoing list of problems, medications, and medication allergies.[90] EHRs must also be able to record a patient's vital signs and smoking status, as well as incorporate laboratory tests.[91] Doctors must have a way to retrieve a list of patients based on specific data, compare medications, submit immunizations to registries, and have access to public health information.[92] There should be means to access information specific to a patient and ways to generate various calculations through data that the doctor can input.[93] Moreover, the user must have control over how to access the information, ways to access it in an emergency, log-off automatically, and create an instinctive log of all actions.[94] The software must also have ways to preserve integrity and authentication, as well as set up a general encryption in addition to an encryption whenever EHRs are exchanged.[95] Further, the regulations give particular criteria for certification for EHRs specifically designed for an ambulatory setting[96] or an inpatient setting.[97] In 2012, HHS added a new section, the 2014 Edition electronic health record certification criteria.[98] The purpose of this section was to clarify the preexisting certification criteria. This simplifies what the vendors need to accomplish within their software before requesting certification.[99]

Vendors must be ONC certified, but having dual certification from another certification process creates buying assurance for potential customers.[100] In 2004, the Certification Commission for Health Information Technology was set up and

---

87 *Id.* § 170.302.
88 *Id.* § 170.302(a).
89 *Id.* § 170.302(b).
90 *Id.* § 170.302(c)-(e).
91 *Id.* § 170. 302(f)-(h).
92 *Id.* § 170.302(i)-(*l*).
93 *Id.* § 170.302 (m)-(n).
94 *Id.* § 170.302(o)-(r).
95 *Id.* § 170.302(s)-(v).
96 *Id.* § 170.304.
97 *Id.* § 170.306.
98 *Id.* § 170.314.
99 *Id.*
100 *Get Certified*, CCHIT, https://www.cchit.org/onc (last visited Oct. 15, 2014).

began certifying EHRs in 2006 to help widen the availability of health information technology.[101] However, in 2014, the Certification Commission for Health Information Technology announced that it will no longer certify EHR software.[102] When they certified, the commission had its own criteria based on "functionality, interoperability, and security."[103] Moreover, there were optional certifications that companies could qualify for as well.[104] The five types of optional certifications were: ambulatory, inpatient, emergency department, behavioral health, and long-term and post-acute care.[105] Each one had its own regulations and criteria that the vendor had to meet in order to be certified. Now, the commission will assist making certain that their software complies with the 2014 Edition requirements.[106]

The ONC has found privacy to be so important with the implementation of EHRs that it has established standards to protect patient information when EHRs are created or transferred.[107] The first four standards that the software must use in order to comply with ONC privacy protections were imposed in 2010. First, the information contained must be encrypted using an algorithm developed by the National Institute of Standards and Technology.[108] According to this Institute, the algorithm is used to protect electronic data by encrypting and decrypting patient information. Once encrypted, the data is converted "to an unintelligible form called ciphertext."[109] Decryption converts the ciphertext back into coherent data.[110] Second, every time that information contained within EHRs is created, accessed, deleted, or in any way changed the user, time, and date must be recorded.[111] Third, there must be verification if "information has not been altered."[112] Fourth, when there is a disclosure for treatment or

---

101 *Our Legacy*, CCHIT, https://www.cchit.org/our-legacy (last visited Oct. 15, 2014).

102 *Id.*

103 *Id.*

104 *Id.*

105 *Get Certified*, *supra* note 100.

106 *Id.*

107 45 C.F.R. § 170.210 (2012).

108 *Id.* at § 170.210(a).

109 FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION 197: ANNOUNCING THE ADVANCED ENCRYPTION STANDARD (AES), COMPUTER SECURITY RESOURCE CTR. (Nov. 26, 2001), *available at* http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

110 *Id.*

111 45 C.F.R. § 170.210(b).

112 *Id.* § 170.210(c).

payment, the date, time, patient, user, and description of the specific discloser must also be recorded.[113]

Effective October 2012, additional privacy standards were added to this regulation. First, an internal audit log must be kept that records the date and time that EHR technology is used or changed.[114] Second, electronic health information contained within the EHRs must be hashed according to an algorithm from the National Institute of Standards and Technology.[115] Hashing is a condensed version of the information contained within.[116] Last, EHRs must include a clock synchronized according to the Network Time Protocol.[117]

B. Failure to Continuously Comply with Certification

The 11th Circuit Court of Appeals heard a case, prior to the implementation of the HHS regulations, which demonstrated the necessity of these certification criteria.[118] In 2009, AvMed, a Florida based corporation which provides health care services, used a form of EHRs accessible through laptop computers.[119] Two of the computers were stolen and because the laptops were unencrypted, the personal information contained within was readily available for use by the thieves.[120] Contained within the laptops was "the sensitive information of approximately 1.2 million current and former AvMed members."[121] With the implementation of the HHS regulations, the ease at which hackers or identity thieves can access this information is severely diminished. Encryption by itself will protect the data even when other protections, such as firewalls, fail.[122]

EHR certification is not indefinite; the ONC can revoke certification if the vendors fail to maintain the certification criteria.[123] HHS has described two types of violations in which certification can be rescinded.[124] Type-1 violations are those in

---

[113] *Id.* § 170.210(d).

[114] *Id.* § 170.210(e).

[115] *Id.* at § 170.210(f).

[116] U.S. DEP'T OF COMMERCE, FIPS PUB 180-4, SECURE HASH STANDARD (SHS) (2012), *available at* http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf.

[117] 45 C.F.R. § 170.210(g).

[118] Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012).

[119] *Id.* at 1322.

[120] *Id.*

[121] *Id.*

[122] *The Role of Encryption in Data Protection*, PGP WEBCAST SUMMARY 9 (2007), *available at* http://download.pgp.com/pdfs/whitepapers/PGP-Cullinane-Webcast_WP_070205_F.pdf.

[123] 45 C.F.R. § 170.565 (2012).

[124] *Id.*

which the vendors violate a law or the integrity of the EHRs.[125] Type-2 violations are noncompliance violations.[126] With type-2 violations, vendors will no longer be in good standing with the ONC and will receive a warning. If they fail to address their lack of good standing, they are warned that their certification will be revoked. There is also an opportunity for the vendors to address a potential false allegation of noncompliance.[127] HHS clearly shows that integrity issues are more serious than noncompliance violations. There is no warning from the ONC and if the vendor is found liable for a type-1 violation they are barred from reapplying for certification for a year.[128] In April 2013 the ONC rescinded certification of two separate EHR software programs developed by the same vendor. The ONC discovered that neither software met the enumerated functionality requirements, at which time it informed the vendor and decided that both programs needed to be retested. Both software programs failed retesting and the ONC revoked the vendor's certification.[129]

It is clear that HHS holds patient privacy in high regard. There are several certification criteria that vendors must comply with in addition to separate privacy criteria for the safe exchange and maintenance of EHRs. Moreover, the regulation is clear that if a vendor fails to maintain these criteria it will lose its certification.[130] However, losing certification is the only current penalty for these vendors. It is obvious that privacy was an issue of significance considered by HHS, but aside from having to wait a year before recertification, there are no deterrents of consequence to ensure that vendors will maintain their certification. Failure to comply with certification can have dire consequences for the patients and the facilities that the vendors serve. Failing to comply means that the EHR software no longer meets each of the certification regulations.[131] These certification criteria are in place to better protect patients and their information. Although not all of the criteria are designed to increase privacy,[132] maintaining every

---

[125] *Id.* at § 170.565(a).

[126] *Id.* § 170.565(b).

[127] *Id.*

[128] *Id.* § 170.565(h)(3).

[129] Rajiv Levinthal, *Two EHRs Fail Test, ONC Revokes Certification*, HEALTHCARE INFORMATICS (Apr. 25, 2013), *available at* http://www.healthcare-informatics.com/news-item/two-ehrs-fail-tests-onc-revokes-certifications.

[130] 45 C.F.R. § 170.565.

[131] *Id.* § 170.565(b).

[132] *See supra* notes 81-99.

certification criterion is important. Failure to maintain the criteria that directly relate to privacy may leave the door open to breach. For example, one criterion is that the EHR must have an automatic log out.[133] If a computer is taken from a medical facility and the EHR does not automatically log out a provider, the information contained within may be accessible.[134] The data may also be accessed externally if the information is not encrypted.[135] For these reasons and despite the aforementioned measures, there still needs to be smarter deterrence in order to protect individual medical information and reflect the importance of maintaining patient health information privacy.

C. Credit Cards: A Look Into An Established Certification Process

Certification is not enough, however, to properly protect patients and their EHRs. This has been illustrated by certification to protect private information in other areas, specifically credit cards. Similar to the certification of EHRs, the Payment Card Industry set up a Data Security Standard,[136] with which credit card companies must comply in order to ensure safe security practices.[137] Similar to EHR privacy standards, the Data Security Standard includes protection, encryption, tracking and monitoring access, access restriction, unique identification codes, regular security tests, and anti-virus software.[138] The security criteria for certification, however, has proven not to be enough to deter companies from failing to continuously comply. From 2006 to 2008 three people hacked data security in places such as Hannaford, 7-Eleven, and Boston Market.[139] Hackers stole information from more than 130 million cards[140] even though

---

[133] 45 C.F.R. § 170.302(q).

[134] Dep't of Health & Human Servs. USA, Ctr. for Medicare & Medicaid Servs., *Security Standards: Technical Safeguards*, HIPAA SECURITY SERIES, Mar. 2007, at 3, *available at* http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf (discussing access control).

[135] *The Role of Encryption in Data Protection*, *supra* note 122.

[136] PCI SEC. STANDARDS COUNCIL, PAYMENT CARD INDUSTRY (PCI) DATA SECURITY STANDARD VALIDATION REQUIREMENTS 1 (2008), *available at* https://www.pcisecuritystandards.org/pdfs/pci_dss_validation_requirements_for_qualified_security_assessors_QSAs_v1-1.pdf.

[137] Edward J. Janger *Locating the Regulation of Data Privacy and Data Security*, 5 BROOK. J. CORP. FIN. & COM. L. 97, 103 (2010).

[138] *Id.* at 104.

[139] Brian Krebs, *Three Indicted in Identity-Theft Case*, WASH. POST (Aug. 18, 2009), http://articles.washingtonpost.com/2009-08-18/news/36839944_1_data-breaches-albert-gonzalez-hackers.

[140] *Id.*

this breach occurred only days after Hannaford had become certified under the Payment Card Industry.[141] Within this brief amount of time, 4.2 million card numbers were taken with 1,800 of the cards used by the hackers.[142]

Although EHRs and the healthcare system seem to mirror data privacy in that they both hold sensitive personal information, they are in fact different on two very important levels. First, the Data Security Standard is a self-regulating regime, meaning that the financial institutions have an incentive to prevent breaches to the software.[143] The institutions are self-regulating because if there is a breach, the majority of the loss will fall on the bank as opposed to the consumer.[144] This incentivizes financial institutions to prevent breaches to avoid having to directly pay the consumers back the money that they lost as a result of the breach. The credit card company regulates itself because if the financial institution detects a breach, they will then presumably take the necessary steps in order to end the breach and stop further damage. This distinction is important because if a self-regulating regime cannot comply with its own certification process, it is indicative of the necessity for EHRs to have a smarter deterrence because they are already not self-regulating. Second, financial breaches are limited and quantifiable. These breaches will stay within other financial institutions and the breached institution can disclose specific numbers, such as card numbers and PINs, to caution their associates. The financial institutions will also be able to clearly assign a cost on how much the consumer was damaged by looking at the exact value that was stolen.

D. Application to EHRs

Due to the immense amount of information that is included within EHRs, it is more difficult to determine where and how it will be used if EHR software is breached. EHRs and healthcare information are not necessarily limited to medical data. EHRs include personal material such as insurance and billing information.[145] They also include health information

---

[141] Linda McGlasson, *Hannaford Data Breach May be "Tip of the Iceberg"*, BANK INFO SECURITY (Apr. 4, 2008), http://www.bankinfosecurity.com/hannaford-data-breach-may-be-tip-iceberg-a-810/op-1. Hannaford received PCI certification on February 27 and news of the breach was announced on March 17. *Id.*

[142] *Id.*

[143] Janger, *supra* note 137, at 109.

[144] *Id.* at 104.

[145] *See* PONEMON INST., *supra* note 25, at 2.

such as genetic issues and disabilities.[146] Moreover, health care facilities are not limited to a single type of institution,[147] such as financial institutions with banks. This also makes it more difficult to warn healthcare facilities of breached and stolen information. Furthermore, healthcare breaches are not as quantifiable. It is difficult to assign a cost to stolen health records.[148] Additionally, EHRs and the healthcare system are also not self-regulating in the same way that financial institutions are. There is less internal incentive to prevent breaches because breaches will not lead to the vendors losing the high costs that financial institutions face.[149]

Merely losing certification is not enough of a consequence for failing to comply. If the vendor loses certification, their EHRs are no longer usable.[150] The medical facilities that spent thousands or even millions of dollars[151] can no longer use the software and the patients' information may no longer be protected. The legal system should be encouraging continued compliance with the certification criteria. For this reason, a deterring monetary penalty is necessary to help protect disclosure of personal health information.

Although failure to comply with certification may not necessarily lead to a breach, allowing vendors not to comply with some of the criteria may lead vendors to believe that some criteria are more important than others. Arguably, the requirements protecting patient privacy may appear more important than the requirements that set up what must be included in EHRs, but each requirement was set up by HHS for a particular purpose and must be treated as equally important.

Disclosure can lead to significant potential concerns such as genetic discrimination, identity theft, and an overall failure in patient faith in the privacy and security of their

---

[146] Peter B. Jensen et al., *Mining Electronic Health Records: Towards Better Research Applications and Clinical Care*, 13 NATURE REVS. GENETICS 395, 397-98 (2012).

[147] *See Hospitals, Nursing Homes, & Other Health Care Facilities*, N.Y. ST. DEP'T OF HEALTH, http://www.health.ny.gov/facilities/ (last updated Sept. 2014).

[148] Jim Landers, *Medical Identity Is Fast-Growing and Dangerous*, DALLAS NEWS (Sept. 16, 2013, 9:00 PM), http://www.dallasnews.com/business/columnists/jim-landers/20130916-medical-identity-theft-is-fast-growing-and-dangerous.ece (noting that breaches can impact the victim's own medical treatment or lead to death).

[149] *Compare* PONEMON INST., *supra* note 25, at 3 (providing that healthcare facilities average $2.4 million in breach costs) *with* PONEMON INSTITUTE, 2011 COST OF DATA BREACH STUDY: UNITED STATES 1 (2011), *available at* http://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf (providing that financial institution breaches have cost as much as $7.2 million to the organization).

[150] Levinthal, *supra* note 129.

[151] *See supra* text accompanying notes 66 and 79.

information. Even with these concerns the necessity of a penalty needs to be examined as supplemental assurance of patient's privacy. There are already safeguards in place, such as mandated encryption as enumerated within the privacy criteria[152] and de-identification as stated in the HIPAA Privacy Act.[153] De-identification means that specific identifying marker must be removed in protected health information, such as, but not limited to, names, e-mail addresses, social security numbers, and device serial numbers.[154] Through examining in place data protection standards and certification it is clear that certification and safeguards are not nearly enough, the vendors need further consequences for failing to comply with data protection standards. Unlike credit card companies, EHRs are not a self-regulating scheme because the vendors do not lose money from breaches. However, merely losing certification does not reflect the importance of privacy that has clearly been placed on EHRs. There needs to be further and smarter deterrence as well.

III. USING AN EXISTING STATUTE TO BOLSTER AND PROTECT PATIENT PRIVACY

Due to the infancy of EHR regulations, the best place to find a civil monetary penalty is to look at existing law. The ideal penalty needs to be smart about what exactly it deters. Due to the vast number of benefits of implementing EHRs,[155] the deterrence should not be harsh enough to deter vendors from creating the software. The penalty, however, should be proportional to the harm, but efficient in its purpose.

A. Existing Law

HIPAA, which states that people who knowingly disclose "individually identifiable health information" will be held accountable,[156] may deter some vendor misconduct. The Supreme Court, however, has set a relatively high standard of mental culpability, holding that knowing disclosure requires "proof of knowledge of the facts that constitute the offense."[157] Moreover, the penalty for violating this statute is equally as

---

[152] *See supra* text accompanying note 108.

[153] 45 C.F.R. § 164.514(a) (2012).

[154] *Id.* § 164.514(b)(2)(i).

[155] *See supra* notes 19-24 and accompanying text.

[156] 42 U.S.C. § 1320d-6(a) (2010).

[157] Dixon v. United States, 548 U.S. 1, 5 (2006) (citing Bryan v. United States, 524 U.S. 184, 193 (1998)).

high, ranging from a fine of $50,000 and the possibility of up to a year of imprisonment to a fine of $250,000 and the possibility of up to a ten-year prison sentence.[158] These penalties, although an effective deterrent are perhaps too harsh for EHRs. These large fines would be in place for a vendor simply failing to maintain a synchronized clock,[159] which may disincentivize vendors from creating EHRs *ex ante*. Further, a failure to comply that may not lead to a breach should not be cause for imprisonment, but may be cause for a fine.

Conversely, the Code of Federal Regulations, with the HIPAA Privacy Rule, has a legal deterrence in place that closely resembles what is ideal for certification breaches. It clearly expresses the magnitude of failure to comply without becoming too harsh. This regulation imposes penalties on a covered entity, which includes "[a] health care provider who transmits any health information in electronic form in connection with a transaction covered under this subchapter."[160]

There are four types of violations under the regulation that are subject to a civil monetary penalty if they occur on or after February 18, 2009.[161] First, if the "covered entity" did not, and could not through reasonable diligence, have known that a provision was violated.[162] Second, if "the violation was due to reasonable cause and not to willful neglect."[163] Third, if the violation was in fact due to willful neglect and was corrected within thirty days after the covered entity knew or could have known about the violation.[164] Last, if "the violation was due to willful neglect and was not corrected" within thirty days after the entity knew or could have known about the violation.[165] These four violations all require lower standards of mental culpability than HIPAA. The regulation defines willful neglect as a "conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision[s] violated."[166] This standard falls below knowledge, but still requires some proof in order to show that the violator actually acted

---

158 42 U.S.C. § 1320d-6(b).
159 45 C.F.R. § 170.210(g).
160 *Id.* § 160.103 (definition of "Covered entity").
161 *Id.* § 160.404(b)(2).
162 *Id.* § 160.404(b)(2)(i).
163 *Id.* § 160.404(b)(2)(ii).
164 *Id.* § 160.404(b)(2)(iii).
165 *Id.* § 160.404(b)(2)(iv).
166 *Id.* § 160.401.

consciously or with reckless indifference. It may even be argued that the covered entity's failure to act is willful neglect.[167]

The monetary penalty that is associated with each one is proportional to the culpability; the lower the mental culpability, the lower the civil monetary penalty and vice versa.[168] The penalty operates on a spectrum that reflects the degree of culpability of the vendor. The first penalty ranges from $100 to $50,000,[169] the second penalty ranges from $1,000 to $50,000,[170] the third penalty ranges from $10,000 to $50,000,[171] and the last penalty must be over $50,000.[172] No penalty may exceed $1,500,000 in one calendar year, meaning from January 1 to December 31.[173]

When deciding the penalty to impose on the vendor within these ranges, the court imposing the penalty may take into account several factors such as (1) "the nature of the violation,"[174] (2) the circumstances of the violation, including the time period, if there was actual harm, and if the victim was prevented from securing health care,[175] (3) the degree of culpability,[176] (4) all history with compliance or violations with the administrative simplification provisions,[177] (5) the finances of the covered entity,[178] and (6) any other matters that may affect justice.[179] These six factors will determine how much, up to the maximum imposed by the regulation, injured parties will receive from covered entities.[180]

These fines are important because the ranges more effectively reflect the degree of culpability while better protecting the injured party. If the violator could not have known that they were violating the provision, they are fined as little as $100.[181] However, the knowledge that they can be fined even if they could not have known[182] is incentive to vehemently try to continuously comply with the regulations. Moreover, the

---

167 *See, e.g.*, U.S. v. Boyle, 469 U.S. 241, 246 (1985).
168 45 C.F.R. §§ 160.404(b)(2)(i)(A), (b)(2)(ii)(A), (b)(2)(iii)(A), (b)(2)(iv)(A).
169 *Id.* §§ 160.404(b)(2)(i)(A)-(B).
170 *Id.* §§ 160.404(b)(2)(ii)(A)-(B).
171 *Id.* §§ 160.404(b)(2)(iii)(A)-(B).
172 *Id.* § 160.404(b)(2)(iv)(A).
173 *Id.* §§ 160.404(b)(2)(i)(B), (b)(2)(ii)(B), (b)(2)(iii)(B), (b)(2)(iv)(B).
174 *Id.* § 160.408(a).
175 *Id.* § 160.408(b).
176 *Id.* § 160.408(c).
177 *Id.* § 160.408(d).
178 *Id.* § 160.408(e).
179 *Id.* § 160.408(f).
180 *Id.* § 160.404.
181 *Id.* § 160.404(b)(2)(i)(A).
182 *Id.* § 160.404(b)(2)(i).

ranges are broad enough for the court to take into account a variety of factors that led to the violation.[183] This allows fines to be imposed entirely on a case-by-case basis and would create fairer penalties because each penalty is decided based on individual factors.

It is important to note that this civil monetary penalty does not go to the victims of the failure to comply (i.e. the patients, whether or not harm actually occurred). Rather, this penalty goes directly to the secretary of the agency imposing the civil monetary penalty to be dispensed of in four ways.[184] The first disposal only applies to penalties that arise either from grants to states for medical assistance programs or the maternal and child health series block grant.[185] Second, any amount of the penalty, which has been taken from a trust fund, must be equally reimbursed to that trust fund.[186] Third, if the claim arises out of a federal health care program, any portion that has been paid by the program will be equally reimbursed to the program.[187] Moreover, anything recovered under HIPAA must be deposited to the Federal Hospital Insurance Trust Fund.[188] Fourth, any remainder must be deposited into the United States Treasury.[189]

B. Applying the HIPAA Privacy Rule Civil Monetary Penalty to EHR Certification

The HIPAA Privacy Rule civil monetary penalty, in operation, is wholly separate from EHR certification criteria. Rather, this civil monetary penalty is imposed if the Secretary of HHS determines that the "covered entity has violated an administrative simplification provision."[190] The only federal regulation mentioned in the definition that may establish requirements or prohibitions that create administrative simplification provisions is Subchapter C within Title 45.[191] The certification criteria developed by HHS is found in Subchapter D of Title 45,[192] so the civil monetary penalty is separate and apart

---

183 *Id.* § 160.408.
184 42 U.S.C. § 1320a-7a(f) (2011).
185 *Id.* § 1320a-7a(f)(1).
186 *Id.* § 1320a-7a(f)(2).
187 *Id.* § 1320a-7a(f)(3).
188 *Id.*
189 *Id.* § 1320a-7a(f)(4).
190 45 C.F.R. § 160.402(a) (2012).
191 *Id.* § 160.302(3).
192 *Id.* § 170.302.

from the criteria. As a result, it can easily be argued that a vendor would not be subject to a civil monetary penalty if they stopped complying with the certification criteria.

This civil monetary penalty must either apply to Subchapter D as well, or Subchapter D must create a similar penalty to impose if vendors stop regulating certification criteria. Subchapter D is not so different from Subchapter C to warrant an argument that the same civil monetary penalties should not apply to both. Subchapter C is the HIPAA Privacy Rule, which was enacted to better protect patient privacy and medical records as well as to provide safeguards for the privacy of personal health information.[193] The certification criteria enumerated within Subchapter D also ensures patient privacy and sets up various ways to protect the sensitive personal health information contained within EHRs. The certification criteria so closely resembles the privacy protections within the HIPAA Privacy Rule that they too should be considered administrative simplification procedures under the definition provided by the regulation. Through this clarification, vendors will be held to the same standard as other covered entities. It is unclear whether EHRs fall under the definition of a covered entity. Although not health care providers, EHRs are implemented by providers and are used to electronically transmit health information in connection with a transaction. However, for clarification, the definition of a covered entity may need to be expanded to include healthcare entities that transmit electronic health information. Moreover, an administrative simplification provision is "any requirement or prohibition established by" various statutes and regulations.[194] EHR certification is a requirement established by a regulation, which must be met in order to receive ONC certification.

Imposing this civil monetary penalty would not preempt victims from filing suits for their own damages. In its current use, the civil monetary penalty is imposed through a civil suit "in the name of the United States," sometimes brought by qui tam.[195] Because the party in the suit is the United States and not the individuals harmed, the patients or medical facilities may bring separate suits with various claims, such as negligence,

---

[193] *The Privacy Rule*, U.S. DEP'T OF HEALTH & HUMAN SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/ (last visited Feb. 1, 2015).

[194] 45 C.F.R. § 160.302.

[195] 42 U.S.C. § 1320a-7a (2011).

breach of contract, restitution, breaching of fiduciary duty, or breaching the good faith and fair dealing covenant.[196]

Breaches are supposed to be reported to HHS. If the civil monetary penalty is imposed, however, there may be reluctance from the vendors to report. Vendors lose nothing for failure to report breaches. This failure to report would inevitably increase the damage to the patients. Consequently, it can be argued that the civil monetary penalty will harm, rather than help, patients through discouraging vendors from reporting breaches to HHS or failing to fix breaches in a timely manner.

Due to this inability to self-regulate, this civil monetary penalty cannot simply be adopted as is; there needs to be a safe harbor provision. A safe harbor provision would incentivize the vendor to report a breach of privacy by putting protections for the vendors in place. The failure to report should be a factor that a judge would consider when determining the amount of the civil monetary penalty to impose. Without the safe harbor there is no guarantee that vendors will report breaches to HHS for fear of having to pay these penalties. Breaches range from external hackers to stolen computers.[197] Vendors should be encouraged, and not afraid, to report these breaches to HHS to better protect patients and to help avoid breaches in the future by determining what caused the breach.

Vendors should also be encouraged to report their own failures if they realized they have stopped complying with the certification criteria before a breach occurs. In this situation, vendors may assume that they can resume complying with certification without informing HHS because there has not been any damage to EHR security. Vendors may be discouraged from reporting this information because even without damage they may still be liable for the high penalties included in the Subchapter C civil monetary penalty. The purpose of reporting the failure to comply is to help HHS rather than to hurt the vendors. HHS should be made aware of these failures to better understand its relatively new certification scheme. This information may help assist decisions in future regulation amendments. In order to help both HHS and the vendors, a safe harbor, such as a "bifurcated notice scheme," should be implemented.[198]

---

[196] Resnick v. AvMed, Inc., 693 F.3d 1317, 1323 (11th Cir. 2012).

[197] Abraham Shaw, *Data Breach: From Notification to Prevention Using PCI DSS*, 43 COLUM. J.L. & SOC. PROBS. 517, 518 (2010).

[198] *See, e.g.*, Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 960 (2007).

This scheme provides five benefits: (1) it helps the vendors determine if they should tell the medical facilities and patients of the breach or failure to comply, (2) better coordinates to warn similar facilities where the stolen information may be used or vendors who may also be targeted, (3) narrowly determines who should be put on notice of the breach or failure to comply, (4) it minimizes ability of the vendor to determine that notice is unnecessary when in actuality it is, and (5) it enforces maintaining certification criteria through both encouraging vendors to approach HHS and coercion to maintain for fear of the penalty.[199]

A bifurcated notice scheme would work as follows: when the vendor notices that they have been breached, with or without damage to patient health information, or when the vendor notices that they have stopped complying with certification criteria, the vendor must inform HHS.[200] HHS will then investigate and determine which patients, if any, should be on notice that their health information may have been compromised. Through this, vendors may avoid putting patients on notice if they discover the failure to comply early enough.[201] HHS will most likely decide, to maintain patient's faith in EHRs, not to inform patients of failing to comply if the failure did not lead to a breach of information. If the vendors follow this bifurcated notice scheme and inform HHS immediately, it will positively influence the court's decision when determining if the civil monetary penalty imposed will be on the higher or lower end of the range. If the vendor does not report the failure to comply, it will influence the same decision to make the penalty higher, which would encourage more compliance with privacy standards.[202]

If the civil monetary penalty is expanded, however, there will be an absurd outcome where the actual thief will pay the same monetary penalty as the willfully negligent vendor. It is possible that if someone steals individually identifiable medical records due to the vendor's willful neglect to uphold and maintain the certification criteria, the actual thief—that is, the person who knowingly steals the records—may potentially pay the same amount in penalty damages as the EHR vendor. HIPAA violators, persons who knowingly use or "obtain[]

---

[199] *Id.*

[200] *Cf. id.* at 960-62 (discussing the notification from a breached entity to the CRA).

[201] *Cf. id*. at 962-63 (discussing that the CRA will determine when consumers will be notified).

[202] *Cf. id*. at 964-65 (discussing the $500 penalty for failure to disclose).

individually identifiable health information,"[203] such as hackers, can pay up to $50,000 in damages.[204] In the lower three tiers of the HIPAA Privacy Rule, covered entities, potentially the EHR vendors, may also pay up to $50,000.[205]

For example, if a vendor's willful neglect caused a failure to comply with the certification criteria, even if it was corrected within thirty days, the door may have been left open within those thirty days for a breach. A hacker could then knowingly take that opportunity and steal medical data. In this case, both the vendor and the hacker could be liable for up to $50,000 in damages, even though the vendor was only willfully negligent and corrected the problem, and the hacker knowingly stole the information. The penalty for the vendor and the hacker should be different here because the mental culpability of each party is vastly different. The vendor in this example corrected the problem within thirty days of the discovery of the problem, even though its own willful neglect led to the problem. Through fixing the problem, it is clear that the vendor did not want to harm the patients whose information is stored by the vendor. However, the hacker knowingly went into the database and took the information to use for his own mal-intentioned purpose. The hacker wanted to harm the patients in order to gain something for himself. For this reason, the penalty imposed on the vendor and the penalty imposed on the hacker should reflect their separate culpability.

Moreover, it cannot be assumed that a court will take care of this because, in the first case, the HIPAA violator will be heard in court by an Article III judge. In the second case, however, because HHS enacted the HIPAA Privacy Rule, violators will presumably be charged in an administrative court. However, the HIPAA penalty also states that violators may be imprisoned for up to a year as well.[206] It is unlikely that this imprisonment is enough to justify the difference between knowingly taking another's personal health information and willfully neglecting certification criteria. With the imposition of the civil monetary penalty, rulemakers should address this issue and either update HIPAA penalties or find another way to distinguish the two penalties. Although the HIPAA penalty is criminal and the Subchapter C penalty is civil, it should still

---

203 42 U.S.C. § 1320d-6(a) (2010).
204 *Id.* § 1320d-6(b)(1).
205 45 C.F.R. §§ 160.404(b)(2)(i)(A), (b)(2)(ii)(A), (b)(2)(iii)(A) (2012).
206 42 U.S.C. § 1320d-6(b)(1).

be addressed that the criminal penalty, with a higher burden, will impose the same monetary amount as the civil penalty.

An 11th Circuit case resulting from a pre-EHR certification breach demonstrated the necessity of the civil monetary penalty even if it is not clear where the breach occurred. The court in *Resnick v. AvMed Inc.* raised a causation issue that would also arise with the implementation of this civil monetary penalty. The court found that in order to find AvMed accountable for the theft, it must be shown that the identity theft occurred due to the laptop theft and not from a breach by a third-party, such as the bank.[207] The identity theft in *Resnick* was purely monetary and not related to the victim's medical history or insurance,[208] so the nexus may not be clearly established.[209] With the implementation of the civil monetary penalty, even if a bank's breach caused the identity theft, the EHR vendor would still pay the penalty if the vendor failed to comply with certification. The reasoning for this is clearly demonstrated in the discussion between the majority and the dissent in *Resnick*. The majority finds it plausible that the stolen laptops caused the identity theft,[210] whereas the dissent finds that there were not enough facts discovered to clearly establish where the identity theft occurred.[211] Presumably, most identity thefts will echo *Resnick* in that it will be difficult to pinpoint exactly where the identity theft occurred, so the civil monetary penalty will further deter vendors from failing to comply in order to avoid paying penalties for identity thefts that were not caused by the vendor's fault.

Identity thefts from EHRs are not limited to economic loss. Through stealing information contained within EHRs, the victims may suffer from insurance fraud or genetic discrimination.[212] Due to these types of identity theft, the nexus between the breach and the theft will diminish because third parties with access to this information are severely limited,[213] as opposed to the number of third parties with access to monetary information.[214]

---

[207] Resnick v. AvMed, Inc., 693 F.3d 1317, 1326-27 (11th Cir. 2012).

[208] *Id.* at 1322.

[209] *Id.* at 1331 (Pryor, J., dissenting).

[210] *Id.* at 1327 (majority opinion).

[211] *Id.* at 1330 (Pryor, J., dissenting).

[212] *See supra* text accompanying notes 31 & 33.

[213] People have one EHR, which limits the number of people who have access.

[214] *Resnick*, 693 F.3d at 1331 (discussing sensitive information received in the mail, credit cards, and how third parties get the plaintiffs' information).

IV. THE ADDED EXPENSE IS SUBSTANTIALLY OUTWEIGHED BY THE INCREASED BENEFITS

There are four separate parties involved with EHRs: the medical facilities, the patients, the vendors, and the government. The implementation of a civil monetary penalty will affect each of these parties. One of the disadvantages of implementing EHRs is the continuous expense of their maintenance on the medical facilities,[215] so it may be unclear if the benefits of implementing a civil monetary penalty will outweigh the costs associated. However, these high expenses paid to set up and maintain the EHR software come directly from the medical facility, whereas the vendors would pay the penalty for failure to comply with certification. But even with the high cost of EHRs, medical facilities will end up saving in the long term. The overall expense of medical care is estimated to decrease by $400 billion a year due to the implementation of EHRs.[216] Medical facilities may be more willing to spend the money to set up EHRs knowing that there is a legal deterrence for the vendors to make sure that they maintain their certification. Without this deterrence, a medical facility may spend up to $10 million to set up an EHR system[217] just for the vendor to stop complying with the certification criteria and have its certification revoked. Additionally, this knowledge may also help to encourage facilities to choose cloud-based vendors once they are aware that some of the security issues are deterred through the civil monetary penalty, which may be beneficial in the future.[218] Cloud-based vendors should be encouraged because it is easier to care for patients nationally and internationally.[219] Moreover, these vendors provide critical management, such as back-ups and maintenance, leaving more time for the facilities to focus on patient care.[220] So, the civil monetary penalty and subsequent deterrence will benefit the medical facilities as such.

The implementation of a civil monetary penalty will also benefit patients by assisting them in reaching an educated decision as to whether they should consent to the use of their information in EHRs. The knowledge that there is a penalty for failing to adequately protect the contained medical information

---

[215] *See supra* text accompanying notes 38-40.
[216] *Analytics in Healthcare*, *supra* note 6, at 3.
[217] *Id.*
[218] *See infra* text accompanying notes 230-32.
[219] Phillips, *supra* note 63, at 25.
[220] Shah, *supra* note 74, at 329.

should ease patients when making their decision. HHS advocates for patients to meaningfully consent to the use of EHRs prior to including their information within them. As part of that advocacy, HHS has developed explicit guidelines for doctors to ensure that patients give meaningful consent to the use of EHRs in the course of their care.

There are six aspects, according to HHS, that patients should consider in order to give meaningful consent.[221] The fifth consideration factor, that EHRs comply with patient expectations, most likely and understandably includes a patient's belief that if he or she agreed to store and transfer his or her records electronically, then those in charge of such records will use due diligence to protect and secure the records.[222] Patients will more likely be comfortable knowing that the vendors securing their records will be held accountable of a breach regardless if individual patients are harmed.[223] Moreover, according to research prepared for the ONC, "if we are to reap the benefits of information exchange, patients must be assured that appropriate technology solutions, business practices, and policy protections will be employed to prevent their information from being used in undesirable ways or to generally impinge upon their rights and civil liberties."[224] This is the heart of meaningful consent. Patients want to be entirely certain that their information is being used properly and that their private information is safe.

The National Coordinator for Health Information Technology stated that there must be clear policies that

---

[221] These aspects are: (1) the decision should be based on education; (2) the patient should satisfactorily look at all material that will help make the decision; (3) understand and agree why health information may be transferred and exchanged; (4) understand that EHRs are not used to discriminate patients and they are not a prerequisite for adequate health care; (5) they comply with patient expectations; and (6) that initial consent to use EHRs is revocable at any time in the future. *Patient Consent for Electronic Health Information Exchange*, HEALTHIT.GOV, http://www.healthit.gov/providers-professionals/patient-consent-electronic-health-information-exchange (last visited Feb. 1, 2015).

[222] Kathryn Marchesini & Joy Pritts, *Meaningful Consent in Electronic Health Information Exchange: A Technology-Centric Approach*, HEALTH AFFAIRS BLOG (Sept. 17, 2013), http://healthaffairs.org/blog/2013/09/17/meaningful-consent-in-electronic-health-information-exchange-a-technology-centric-approach/.

[223] Pear, *supra* note 50, at 3 ("Until people are more confident about the security of electronic medical records . . . it's vitally important that we err on the side of privacy." (internal quotation marks omitted)).

[224] MELISSA M. GOLDSTEIN, J.D. & ALISON L. REIN, M.S., CONSUMER CONSENT OPTIONS FOR ELECTRONIC HEALTH INFORMATION EXCHANGE: POLICY CONSIDERATIONS AND ANALYSIS 1 (Mar. 23, 2010), *available at* http://www.healthit.gov/sites/default/files/choicemodelfinal032610.pdf.

"strengthen existing protections"[225] for E-Health. A deterring civil monetary penalty will do exactly that; it will strengthen the existing protections enumerated within EHR certification criteria. Further, in 2012, it was estimated that 1.85 million people were victims of medical identity theft.[226] Imposing the civil monetary penalty and holding the vendors liable for all failures to comply, regardless of breaches or harm, will presumably lower this number, making it less likely that patients' sensitive information will be compromised. For these reasons, the penalty will benefit patients.

The civil monetary penalty will benefit vendors even though they are the ones who will ultimately pay the fine. Under the American Recovery and Reinvestment Act of 2009, companies that comply with goals outlined by the ONC may receive subsidies from the Secretary of HHS.[227] The purposes of this federal incentive are to protect patient health information, reduce health care costs, improve coordination between different medical practices, and improve the overall effectiveness and quality of health care services.[228] EHRs do all of this,[229] so the vendors who implement EHRs and comply with the certification criteria are able to receive the federal incentive payment. Through this payment, the direct expense that vendors must pay is lessened.

The civil monetary penalty will also assist with cohesion between different EHR vendors.[230] A major challenge with the use of EHRs developed by many different vendors is health information exchange, that is, that different software cannot communicate with each other.[231] This is a problem because if a patient goes to a doctor who uses one vendor but then goes to a second doctor who uses a different vendor, the second doctor will not have access to records from the first doctor until they are safely transferred. Likewise, once the second doctor is finished with the patient, the information that he collected will not be in the record that the first doctor has until the information is once again transferred and combined. Right now, this is a huge cost of EHRs. Medical facilities are spending millions of dollars to use

---

225 *Id.*

226 *See* PONEMON INST., *supra* note 31, at 1.

227 42 U.S.C. § 300jj-31 (2009).

228 *Id.* § 300jj-11.

229 *See supra* text accompanying notes 88-95.

230 *See generally* Jensen et al., *supra* note 146, at 403 (discussing the developments towards interoperability).

231 Adler-Milstein & Jha, *supra* note 54, at 1695.

them,[232] but different facilities cannot even talk to each other easily regarding one patient.[233]

It is logical that both the cohesive vendors and the software, which creates the cohesiveness, will fall under Subchapter D, so they would be subject to the civil monetary penalty. Software regarding EHR storage and transfer will need to fit the criteria in Subchapter D to receive certification and then would have to comply to avoid decertification and the civil monetary penalty. Moreover, these vendors and software, more so than the vendors and software existing today, will need this protection. EHRs today have limited reach. It is presumably more difficult for a hacker in California to access EHRs in a New York office, and even more so if the EHRs are on-premise. With vendor cohesion, all EHRs will turn into cloud-based records because they are easier to use for multiple facilities,[234] making it easier for anyone anywhere to access any records. The implementation of the civil monetary penalty will help to facilitate the cohesion between vendors. The civil monetary penalty will inevitably lead to better EHR vendors because they will be fiscally responsible for their actions. This would then lead to better EHRs because breaches would occur less. The next step is cohesiveness between vendors,[235] which would then require cloud-based EHRs.

Patients will again be more comfortable with the fluidity created by cohesion between vendors because of the civil monetary penalty. They will feel confident knowing that the people who are in charge of the health information exchange and their personal health information are liable for breaches, regardless of the type of violation, and that the vendors must uphold certain criteria or be penalized.

Additionally, the imposition of the civil monetary penalty will put patients at ease with the privacy concerns surrounding cloud-based records.[236] Due to the increased amount of breaches in this model, there is more incentive for the vendors to continuously comply with certification, for fear of substantial penalties for each breach. This may even encourage the vendors to impose additional safety measures. Further, this will help protect patient privacy if the cloud-based servers are kept

---

[232] *Analytics in Healthcare*, *supra* note 6, at 3.

[233] Adler-Milstein & Jha, *supra* note 54, at 1695.

[234] duPont et al., *supra* note 77, at 402.

[235] *See generally* Jensen et al., *supra* note 146 (discussing the developments towards interoperability).

[236] *See supra* text accompanying notes 67-76.

outside of the United States. Although the vendors will have to comply with the foreign privacy laws for maintaining the server,[237] they will still be subject to the certification criteria and the civil monetary penalty. So, even if foreign privacy laws are less strict, the vendors will be responsible for the minimum safeguards provided within the HHS regulation.

HHS implemented the certification regulations[238] to make certain the EHRs, which contain the personal information of patients, met criteria that the agency deemed important. Although the criteria are both administrative and clinical,[239] the vendors should show the same amount of care to comply with each criterion. Imposing the civil monetary penalty would disincentivize the vendors from deviating from the agency regulation. Moreover, if the civil monetary penalty was imposed, the fine would be directed to the Secretary of HHS.[240] It would partly be used to reimburse HHS for the subsidy provided to that vendor[241] as part of the American Recovery and Reinvestment Act of 2009.[242] Imposing the civil monetary penalty would lead to more compliance with HHS' certification criteria regulations and more protection of patients' medical data.

CONCLUSION

E-Health and EHRs have greatly expanded over the last fifty years. The implementation of EHRs has led to increased safety, fewer mistakes, and cheaper healthcare. However, privacy continues to be a major concern. Privacy of patient medical information is so important to lawmakers that they have an entire rule, the HIPAA Privacy Rule, outlining specific ways to safely ensure that privacy will be maintained while transferring health information. Further, in order to make certain that EHRs, which have the added responsibility of storing patient information, continue to maintain patient privacy, HHS implemented numerous criteria that vendors must comply with in order to receive certification as well as several privacy standards.

As shown through other forms of certification, this is not enough. There needs to be a legal deterrence to help maintain the

---

237 Das et al., *supra* note 69, at 22.
238 45 C.F.R. § 170.302 (2012).
239 Jensen et al., *supra* note 146, at 397-98.
240 42 U.S.C. § 1320a-7a(f) (2011).
241 *Id.* § 1320a-7a(f)(3).
242 *Id.* § 300jj-31.

integrity of EHRs and the integrity of the private medical data. HHS should either expand the civil monetary penalty included within the HIPAA Privacy Rule, that does not encompass the certification criteria, or consider implementing a similar rule that will solely apply to certification. Vendors need an incentive to report breaches to HHS or else we run the risk that they will handle these internally to the detriment of patients. A safe harbor provision should also be included within this civil monetary penalty stating that if vendors report all breaches to HHS, it will reflect favorably on the vendors when a decision as to the amount of the penalty is made. Moreover, allowing HHS to deal with breaches internally will prevent unnecessary patient notification when a breach may not affect the patient's individual EHR. Even though a civil monetary penalty will be a cost to vendors, the ultimate benefit substantially outweighs the cost. Not only does the vendor benefit, but patients and medical facilities benefit as well due to the additional incentive to continuously comply with certification and the dividends that will follow for patient privacy. Implementing this civil monetary penalty will benefit EHRs, vendors, healthcare providers, and, most importantly, patients.

Mallory Turk[†]

[†] J.D. Candidate, Brooklyn Law School, 2015; B.A., Binghamton University, 2012. Thank you to Jeannette Russoff and Professor Edward Janger for their comments and ideas throughout the writing process and to the *Brooklyn Law Review* for their continued effort. Most importantly, I would like to thank my family for their endless love and support. This note is dedicated to the memory of my grandfather.